AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
4:22 MJ 5250 NAB	11/02/2022 at approx. 10:00 AM	Device was in USPIS possession.

Inventory made in the presence of :
The inventory is not yet complete.

Inventory of the property taken and name of any person(s) seized:

On November 2, 2022, I gave the Device to the USPIS forensic computer analyst in St. Louis, MO for imaging and analysis. The Device was locked by a passcode, which required assistance from the national forensic laboratory. The analysis is not yet complete and is ongoing.

On 11/3/2022, this warrant return was submitted by reliable electronic means to the undersigned U.S. Magistrate Judge who signed and issued it in the referenced case. By reliable electronic means, this returned warrant is forwarded to the Clerk of Court for filing, with a copy to the officer who returned it.

NANNETTE A. BAKER
U.S. MAGISTRATE JUDGE
11 / 3 / 2022

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: 11/03/2022

Executing officer's signature

Postal Inspector Kory Kuba
Printed name and title

ATTACHMENT A

The property to be searched is an Apple iPhone, believed to be an Apple iPhone 8, dark gray in color (hereinafter "the Device"). The Device was seized from Works following his arrest by the University City Police Department (UCPD) on September 20, 2022, is currently located at the USPIS office located at 1106 Walnut St, St. Louis, MO 63199.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Device described in Attachment A that relate to violations of Title 18, United States Code, Sections 472 (Uttering Counterfeit Obligations or Securities), 1341 (Mail Fraud), 1343 (Wire Fraud), 1344 (Bank Fraud), 1349 (Conspiracy to Commit Mail and Wire Fraud), 1708 (Theft or Receipt of Stolen Mail Matter) and 371 (Conspiracy to Commit Offenses) and involve Deantie Works, "Nisha" LNU (believed to be Juanisha Jennings), Kenneth Woods, and others known and unknown, from June 2018 to Present, including:

a. Any communication related to the theft, purchase, sale, and/or receipt of checks from the mail service, mobile applications, coconspirators, or from others unknown.

b. Any communication related to altering checks, including products, items, electronic equipment, or other means used to alter checks.

c. Any communication related to locations where checks have been stolen, bought, sold, acquired, and/or altered.

d. Any communication involved in the leading, operating, managing, directing, instructing, scheduling, and/or participation in the criminal organization of individuals known and unknown concerning stolen, altered, forged, counterfeited, and/or fabricated checks.

e. All photographs relating to bank receipts, bank cards of deposits or withdrawals, and stolen, altered, forged, and/or counterfeited checks.

f. Any information related to tools or techniques associated with theft, fraud, or financial crimes.

g. All bank records, checks, credit/debit/prepaid card information, account information, and other financial records.

h. All contacts and personal identifying information, including full name, email addresses, physical addresses, telephone numbers, screen names, and other personal identifiers.

i. All logs of activity showing the user's interaction with the Device, GPS coordinates, incoming and outgoing calls, message content, calendar entries, movements, web searches, Bluetooth connections, Wi-Fi connections, and any other metadata associated with the device from June 2018 through the date this warrant was signed.

j. All photos and videos uploaded by the user and all photos and videos uploaded by any user that have that user tagged in them from the June 2018 through the date this warrant was signed, including Exchangeable Image File ("EXIF") data and any other metadata associated with those photos and videos.

k. All social media profile information, profile information, screen names, vanity names, news feed information, status updates, videos, photographs, articles, notes, friend lists, groups and networks of which the users is a member, future and past event postings, rejected friend requests, comments, gifts, pokes, tags, and information about the user's access of those social media applications.

l. All records or other information regarding the devices and internet browsers associated with, or used in connection with, that user ID, including the hardware model, operating system version, unique device identifiers, mobile network information, and user agent string.

m. All other records and contents of communications and messages made or received by the user from the June 2018 through the date this warrant was signed, including all messenger activity, private messages, chat history, video and voice calling history, and pending "unsent" messages.

n. All "check ins" and other location information.

o. All IP logs, including all records of the IP addresses that logged into the account.

p. The types of services and apps utilized by the user.

q. The means and source of any payments associated with the service or the Device, including any credit card or bank account numbers.

r. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.